Blockchain-based Two Factor Authentication on Web Application

By Marsha Chikita Intania Putri

WORD COUNT 4745
TIME SUBMITTED 01-MAY-2020 02:37PM
PAPER ID 58184161

Register 6 (1) 2020 pp. 1-5
Jurnal Ilmiah Teknologi Sistem Informasi (Scientific Journal of Information System Technology)
ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)
Available online to www.journal.unipdu.ac.id
Unipdu
S2-Accredited – SK No. 34/E/KPT/2018
Journal Page is available to www.journal.unipdu.ac.id:8080/index.php/register

Blockchain-based Two Factor Authentication on Web Application

Marsha Chikita Intania Putri [1], Parman Sukarno [2], Aulia Arif Wardana [3]

[1] *Informatics Engineering, Telkom University, Bandung, Indoneia*
[2] *Informatics Engineering, Telkom University, Bandung, Indoneia*
[3] *Informatics Engineering, Telkom University, Bandung, Indoneia*
email: [1] marshachikita@student.telkomuniversity.ac.id, [2] psukarno@telkomuniversity.ac.id, [3] auliawardan @telkomuniversity.ac.id

ARTICLE INFO

Article history:
Received 24 January 2020
Revised 30 April 2020
Accepted 2 December 2020
Available online xxx

Keywords: [Key word heading]
Two factor authentication
Blockchain
Token
Third-party

IEEE style in citing this article: [citation Heading]
F. Fulan and F. Fulana, "Article Title," Register: Jurnal Ilmiah Teknologi Sistem Informasi, vol. 6, no. 1, pp. 1-10, 2020. [Fill citation heading]

ABSTRACT

Authentication is a method for securing an account by verifying user identity by entering an email or username with a password. One type of authentication is two factor authentication. The workings of two factor authentication work the same as authentication in general, namely by entering an email or username with a password. However, two factor authentication requires additional information that must be inputted by the user. Additional information can be in the form of tokens or one-time passwords (OTP). Two factor authentication generally stores user data in a centralized database. In addition, two factor authentication generally still uses third-parrty services to generate token or OTP so that it is very vulnerable to data hacking or snooping by an attacker. Therefore we propose a two factor authentication method with blockchain technology where data storage on blockchain technology is not centralized but distributed without using third-party services as a token generating tool that is implemented in a web-based application. The results obtained from the analysis of the system that has been made by implementing two factor authentication on the blockchain is an appropriate solution to avoid data loss if at any time an attacker attacks the centralized third-party system.

1. Introduction

Authentication is a way to secure an account by verifying user identity which usually a combination of username or email with password to gain access to the account. User tends to use the same password on various platforms [1]. User also tends to use passwords that are easy to remember [2]. Both of these can be categorized as password with low security level. With a low level of security, it will be easier for attacker to hack password and take over user account. According to Verison Data Breach report in 2016, more than 63% of hacking success was caused by compromised credentials [3]. Therefore, new authentication technology was made with more sophisticated security system compared to password authentication or single-factor authentication called two factor authentication of 2FA.

2FA is an additional security layer that is used to ensure only the account owner who can access the account. 2FA is almost the same as single-factor authentication where user enters combination of username or email with password, only user does not directly logged in to their account but has to enter additional information which is usually in the form of token or one-time password (OTP). This method is safer compared to single-factor authentication. Although two factor authentication is considered safer than ordinary authentication, two factor authentication also has weakness. The weakness of two factor authentication is that the system still store the data in a centralized database [2][4]. A system that has centralized database has security risk where the database can be hacked by attacker that cause damage and even loss of large amount of data [3]. Another weakness is that two factor authentication requires

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

third-party to generate the token where the third-party is always be the target of an attacker [2] [4] [5]. However, the weaknesses of two factor authentication can be overcome by technology called blockchain.

Blockchain is a technology consist of many nodes that is connected to each other in a network and can be used to store data in a decentralized system where the data stored on each node is exactly the same and is imutable or permanent. Blockchain technology was found by S. Nakamoto and was first implemented in 2008 and 2009 as the core component of Bitcoin cryptocurrency [6]. The data stored in a distributed system makes it difficult for attacker and almost impossible to make changes to the data stored in a block in blockchain. Furthermore, performing two factor authentication using blockchain does not require third party to generate token [2][7]. Therefore, this paper proposes a blockchain-based two factor authentication technology without third-party where the token is generated by web server and sent to blockchain. Later, this system can be applied on a web application to protect user data from being stolen by attacker and make the system safer.

2. Literature Review

2.1. Related Work

Longfei Wu et. all in paper [7] proposed a two factor out-of-band authentication scheme method for blockchain infrastructure-based IoT devices to prevent collusion on a centralized server. The weakness of this paper is that it does not emphasize the two factor authentication used. The blockchain in this paper is used only to secure its IoT system, while the two factor authentication security on this system is still insecure. And the other weakness is the authentication still use third-party services.

Eman et. all in the paper [11] proposed 2FA framework method with OTP-SMS built on the blockchain network to overcome various kinds of attacks including MITM and third-party attacks. The paper explained the OTP that had been generated would be encrypted and hashed to avoid snooping. But the system in this paper still use OTP-SMS where the system is centralized so it is still not safe because centralized systems have a greater chance of being hacked than distributed systems.

The problem raised in Varun Amrutiya et. all paper [2] is that tokens on 2FA are generated by centralized third-parties where usually trusted third-parties are always under security threats. Therefore, the author proposed 2FA method to use blockchain without using third-party by adding openSSH extra security layer. The advantage of this system is that it does not require third-party so it does not need to be integrated with SMS or mailing systems. But because this system does not use third-parties, the author made a system where tokens for 2FA are generated by the user themselves. The token which consists of six digits will then be saved to the blockchain, so if later at another time the user wants to log into the system, the user must enter the six digit token that has been entered before. So, it does not suit the characteristic of token which should be a one-time password that can only be used once.

In order to cover the weakness of the systems described above to obtain a secure authentication system, we will create blockchain-based two factor authentication system without third-party that will be applied to web applications where tokens used for two factor authentication will be generated automatically by web server and of course it will match the characteristic of a token which can only be used once. For more details, it will be explained in the later section.

2.2. Authentication

Authentication is the process of identifying a user identity and confirming whether the user is authentic or not. Authentication of someone is done to confirm the identity of that person. On a computer system, authentication is done in the login process where the user requests access rights to the computer system to be able to use a particular account. Login to a computer system is done by entering a combination of email or username with a password so that the user has the right to access an account. In the user authentication process, there are three components involved, namely:

1. Supplicant

   Supplicant is a client or user of an authentication that provides their identity as proof that the person is authentic or authentic.

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

2. Authenticator

Authenticator can also be referred to as a server that provides resources and other needs to the client and serves to ensure the identity of users who carry out authorization.

3. Security Authority

Security authority can also be called a database that is used to store credential data from users. In addition, the security authority also serves to check the credentials of users.

One type of authentication is single-factor authentication or often known as password-based authentication. In its application, password-based authentication still cannot accommodate the security and confidentiality of account owner data [16][17][18][19][20]. Therefore, other types of authentication are made, namely two-factor authentication and multi-factor authentication.

2.3. Two Factor Authentication

Two factor authentication is an authentication technology created after single-factor authentication. Two factor authentication or commonly known as 2FA is an additional layer of security in authentication process to ensure that only account owner can access the account. Similar to single-factor authentication where users are required to enter a combination of email or username with password, but there is a slight difference. In single-factor authentication, after the system confirms that the email or username and password entered is correct then user can get access to an account. But using two factor authentication, user does not immediately granted access even though the combination of email or username and password entered is correct. 2FA system will ask for additional information usually in the form of token or one-time password (OTP)

One-time password (OTP) is an authentication method where the user enters a random and automatically generated series of numeric or alphanumeric characters. Each password generated from this OTP system can only be used once for a limited time. OTP can protect the system from passive attacks, but cannot protect from active attacks [8]. Passive attacks include keyloggers [9], Snooping and Eavesdropping [10]. The OTP method has characteristics that make it difficult for an attacker to hack a password. There are two characteristics of OTP:

1. Limited time span

Passwords generated by tokens can only be used for a limited time. If the password is not used within the specified time span, then the password will expire. If the one-time password has expired, the system will send back a new one-time password for user input. Usually the validity period of passwords in OTP is 3-6 minutes [8].

2. Can only be used once

The password generated by the system can only be used once, which is why this password is called a one-time password. If a password has been used, it cannot be used again.

2.4. Blockchain

Blockchain consists of several computers or called nodes that are connected to each other in a network. Each node that is connected stores data or records a transaction that occurs in the blockchain system so that the data in the blockchain is scattered. Data that has been stored in the blockchain system is imutable or fixed, so the data that has been recorded can no longer be changed.

The difference between blockchain and database server is in the way data is stored. Database servers store data centrally, so if an attacker is able to hack the server, there will be damage and even data loss in very large amounts. Data on the blockchain is scattered across all nodes that are connected, so that the attacker is more difficult to hack the blockchain system.

Consensus is the main component of the blockchain that is responsible for reaching agreement in a distributed system. Blockchain has several consensus methods, including proof-of-work (PoW) and proof-of-stake (PoS). Bitcoin uses the proof-of-work (PoW) consensus method which is very important for maintaining consistency and synchronization of data between nodes [15]. Whereas Ethereum uses a

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

proof-of-stake (PoS) consensus method to maintain data consistency. Also there is also a term called mining in blockchain, which is to solve the cryptographically hard puzzle problem where each miner (node connected to the ethereum blockchain network) who successfully resolves the problem can add a block to the ethereum blockchain and will be rewarded in the form of ether [14].

Ethereum is a global platform with a decentralized system for money and other applications. Ethereum was created in 2014 by Vitalik Buterin who was previously involved in Bitcoin [13]. Ethereum is divided into two after hacking in a decentralized autonomous organization (DAO) namely Ethereum (ETH) and Ethereum Classic (ETC). With Ethereum, users can write code that can set digital values, run it according to what was written using program code, and can be accessed throughout the world [12]. Ethereum provides a platform for building distributed applications that connect stack holders directly to achieve transparent and zero-dependency. Although Ethereum has the same core system as Bitcoin, but both have different goals and abilities [3]. Ethereum can change all centralized systems into distributed systems with unique programming capabilities. Therefore, we use ethereum blockchain in this two factor authentication system.

3. Proposed System

3.1. System Overview

An overview of the system can be seen in Figure 1 where user accesses a distributed application (dApp) which has web3js, registration smart contract, and 2FA smart contract while dApp is connected to the ethereum blockchain.

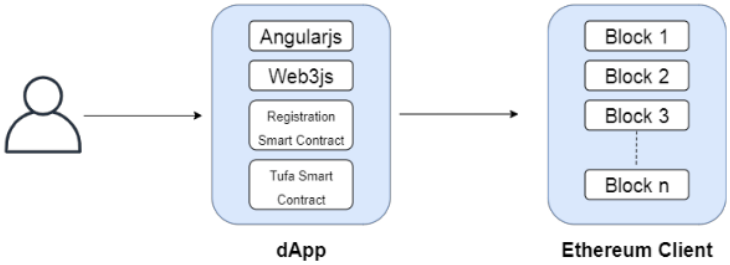

Figure 1. 2FA with Ethereum Blockchain

Distributed application (dApp) is a component that is used to create an ethereum blockchain based application. Dapp consists of a collection of smart contracts needed to build a system. In the system that will be created in this paper requires two smart contracts, first is registration smart contract used to register or create an account the second is tufa smart contract used for two factor authentication. Besides smart contract, there is web3js on dApp, a web library that is used to work on smart contracts and is integrated with nodes on the ethereum network. Blockchain-based two factor authentication uses web3 provider as a bridge for dApp and ethereum blockchain to communicate. To see more detail how dApp can communicate with the ethereum blockchain can be seen in Figure 2.

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

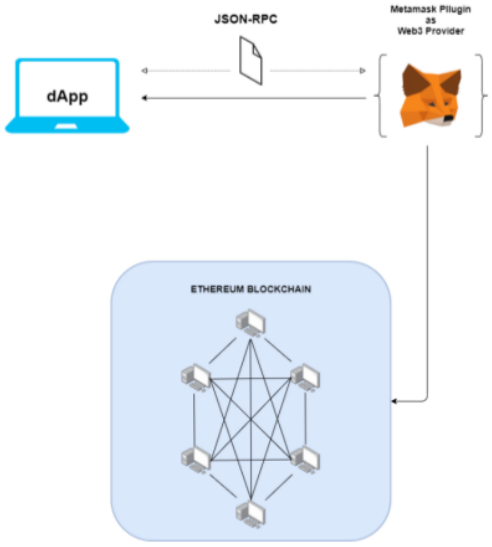

Figure 2. Web3 Provider for Blockchain-based 2FA

To find out in more detail how web3js works with ethereum blockchain can be seen in Figure 3. Web3js is divided into two parts named Application Programming Interface (API) and core. Blockchain-based two factor authentication on web application use API to make and carry out transactions according to the functions exist in the smart contract. Then the transaction will be executed in core by signing on the transaction that has been made using a private key wallet owned by each user. The signed transaction will then be forwarded to the blockchain network and recorded in a block in the node.

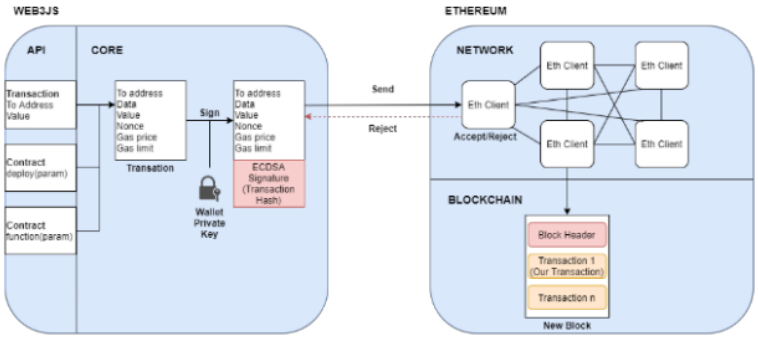

Figure 3. Transaction Between Web3js and Ethereum Blockchain

Before transactions are recorded in blocks on each node connected in the ethereum blockchain network, signed transactions must move from web3js to the blockchain network. To do this, signed transactions will be forwarded to the blockchain network using an object notation called JavaScript Object Notation (JSON). In Ethereum-based applications there is an object notation that has a function similar to JSON called JSON-RPC. This system uses JSON-RPC to distribute data or information from front-end to back-end or vice versa.

3.2. How The System Work

To be able to authenticate, user has to create an account by registering email and password. Before registration data is stored to blockchain, e-mail and password is checked. Emails are checked to have the appropriate e-mail format. If invalid, error message will be displayed. Conversely, if the email is

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

valid, then proceed with checking the password. Registered password must be at least eight characters long, have uppercase letters, punctuation marks, and numbers. If password that will be registered does not meet these conditions then error message will be displayed. If valid, then check again whether the email to be registered already exists on the blockchain. If email is already registered in blockchain, then user is recommended to register with another email, but if the email is not registered yet then the data will be stored into the blockchain and the account is successfully created. More details can be seen in Figure 4 where the account registration flow is illustrated in the form of activity diagrams.

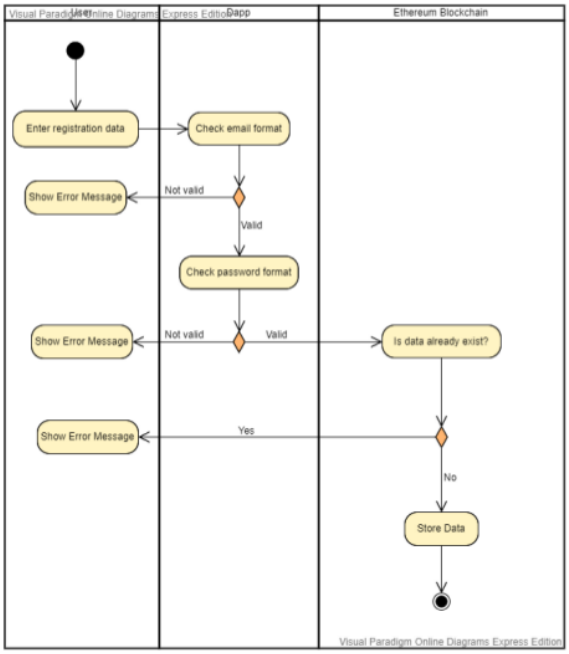

Figure 4. Registration Activity Diagram

The flow of login with two factor authentication can be seen in Figure 5. The user enters the email and password, then dApp will check whether the entered email already registered in the blockchain. If it is not registered yet, an error message will be displayed. Conversely if the email has been registered, dApp will create a session and generate token followed by a page move to the 2FA verification page. On the 2FA verification page, user must click the authenticate button to do two factor authentication. After that, the token that has been generated by dApp will be sent to the blockchain to be stored. Dapp will check if the token stored on the blockchain is the same as the generated session token. If they are not the same an error message will appear, if true then user access is granted.

http://doi.org/10.26594/register.v6i1.idarticle

7
ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

Figure 5. Login Activity Diagram

4. Results and Discussion

The system that we made can be seen in Figure 6. The application that we made has a role-based access control where only the super admin and admin can create a new account. Accounts that have super admin roles can create other super admin accounts and admin accounts. Accounts that have admin roles can only create staff accounts, and staff accounts can not create accounts. Super admin can login for the first time by using default email and password. Later in this section, we will discuss more on the authentication system rather than the registration system.

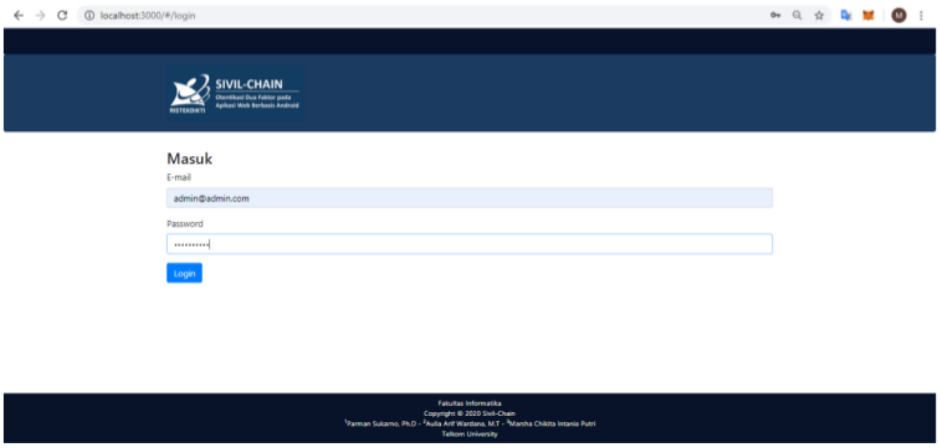

Figure 6. Login Page Sivil-Chain

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

Two factor authentication on our system is different from two factor authenticity in general, where users are usually required to input tokens obtained from emails or phone numbers generated by third-parties. But on our system, user does not have to input the token themselves but after the login button is clicked by user, web server will automatically generate a token and will be sent to blockchain after user clicked the authenticate button in web application. Thus, the system that we made does not require a third party. The algorithm for generating tokens can be seen in Figure 7 as follows:

```
const min = 1;
const max = Math.pow(10, 15);
function getRandomInt() {
  return Math.floor(Math.random() * (max - min + 1)) + min;
}

let newToken = getRandomInt();
while(previous == newToken) {
  newToken = getRandomInt();
}
return newToken;
```

Figure 7. Generating Token

The generated token consist of 15 digits and will be hashed using SHA-256 algorithm and will then be stored temporarily in the session struct. Session struct contains email, user ethereum address, role, token, and token verification. Verification tokens are set to false by default. To perform two factor authentication, the user must click on the authenticate button, then the hashed token is sent to the blockchain using ethereum address of the user to be stored. The web server will compare whether the ethereum address that made the transaction or save the token into the blockchain has the same address as the address that is temporarily stored in a session struct. If the user ethereum address match, then token verification value will set to true and access to the website is granted. With token delivery system as described above, the possibility for attacker to alter or get the token to steal the data is difficult.

In addition to hashing as explained above, we also check the tokens on our system whether the generated tokens are not the same, so that authentication can only be used once to handle the problems written in section 2. Within one second, the web server can generate a maximum of 3164 tokens. We took a sample of 50 tokens which can be seen in Table 1. From as many as 50 tokens it can be seen that the values are not the same. So, the token on our system suits with the characteristics of token where the token can only be used once.

Table 1. Tokens generated by web server before being hashed

No	Token	No	Token
1	937958657735373	25	426297562076200
2	470036333865346	26	908955579532084
3	115031583205754	27	423962133614487
4	377067683320765	28	349735920336760
5	718612641803904	29	540624218275875
6	631742379053109	30	350996926605566
7	693206062001448	31	608973671506405
8	415188786313670	32	194260291133290
9	296241407917450	33	286803324229088
10	471777418953950	34	353155613119854
11	169184427064309	35	436784166505726
12	614017115989873	36	874119779311636
13	285434286811499	37	853868873812529
14	701471238979732	38	710522123418245
15	981508730467085	39	966704114807793
16	349627895040720	40	478955574651406

http://doi.org/10.26594/register.v6i1.idarticle

F. Fulan, et. al./Register 6 (1) 2020 pp. 1-5
ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

17	729629535852415	41	320557690112697
18	779078127703149	42	696624591166778
19	518187805351323	43	518975964536636
20	312510028340080	44	185396696097843
21	266694262643627	45	764082217817079
22	673336797462206	46	278739748115596
23	587177425255582	47	708432464198642
24	912173666416864	48	807704056488856
25	426297562076200	49	561524805179806
26	908955579532084	50	679256723429249

5. Conclusions

Weaknesses in the two factor authentication using the blockchain from previous studies included at section two still using third-parties to generate tokens and some are not using third-parties to generate tokens however the generated tokens do not comply with the token characteristic that should only can be used one time. The system that we made aims to cover the weakness in existing systems so that a secure authentication system is obtained. After analyzing the system that we made, there are several conclusions obtained:

1) The token is being hashed before sent to the blockchain to prevent attacker from altering or steal the token and protect user personal data.
2) Web server can generate up to 3164 tokens in one second and all of them are different tokens, so it suits the token characteristic where token can only be used once in one authentication process.
3) By implementing two factor authentication with blockchain technology without using third-party is an appropriate solution to avoid data loss if at any time an attacker attacks the centralized third-party system.

In addition to the conclusions above, during the process of making the system we also get the conclusion that if the smart contract made has been deployed into a blockchain, then to add or change the code in the smart contract can still be done however the data that has been stored will be lost and smart contract have to be deployed from the start. We suggest to readers if you want to use the blockchain to build dApp it should be analyzed and ascertain in advance whether the code written to create a smart contract will definitely not change again in the future.

7. References

[1] Anusha Govind Bangi B. M Sanjana Archana B.S, Ashika Chandrashekar. Survey on usable and secure two factor authentication. *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017.

[2] Pranjal Priyadarshi Ashutosh Bathia Varun Amrutiya, Siddhant Jamb. Trustless two factor authentication using smart contracts in blockchain. *International Conference on Information Networking (ICOIN)*, 2019.

[3] Rajneesh Gupta. *Hands-On Cybersecurity with Blockchain*. Packt Publishing Ltd, Birmingham, 2018.

[4] Waqar Asif Hassaan Khaliq Qureshi Muttukrishnan Rajarajan Syed Muhammad Danish, Marios Lestas. A lightweight blockchain based two factor authentication mechanism for lorawan join procedure. *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019.

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

[5] Ben Cresitello Dimar. Application of the blockchain for authentication and verification identity. *Independent Paper*, 2016.

[6] Miguel Pincheira Koustabh Dolui Fabio Antonelli Muhammad Salek Ali, Massimo Vecchio and Mubashir Husein Rehmani. Application of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorial*, 2018.

[7] Wei Wang Longfei Wu, Xiaojiang Du and Bin La. An out-of-band authentication scheme for internet of things using blockchain technology. *International Conference on Computing, Networking, and Communications (ICNC)*, 2018.

[8] Oki Indrasto. Implementasi dan analisis sistem autentikasi menggunakan metode otp (one time password) pada server snmp (simple network management protocol). https://openlibrary.telkomuniversity.ac.id/home/catalog/id/131743/slug/implementasi-dananalisis-sistem-autentikasi-menggunakan-metode-otp-onetime-password-pada-server-snmp-simple-network-managmentprotocol-.html, 2014. [*last accessed* 22-October-2019].

[9] Sonam Mahajan Manpreet Kaur Gill Manju Dandi Jatinder Teji, Rimmy Chuchra. Detection and prevention of passive attacks in network security. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, 2013.

[10] Soneye Adeyinka Vu Cong Hoan. An analysis of collaborative attacks on mobile ad hoc networks. *Master Thesis Blekinge Institute of Technology*, 2009.

[11] Eman T Alharbi, Daniyal Alghazzawi. Two Faactor Authentication Framework Using OTP-SMS Based on Blockchain. *Transaction on Machine Learning and Artificial Intelligence*, 2019.

[12] Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger Byzantium Version 7e819ec. *Ethereum Yellow Paper*, 2019.

[13] Vitalik Buterin. A next-generation smart contract and decentralized application platform. *Ethereum White Paper*, 2014.

[14] A. D. Yulianto, P. Sukarno, A. A. Wardana and M. A. Makky. Mitigation of Cryptojacking Attacks using Taint Analysis. *4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2019.

[15] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[16] Hyun-A Park, Jong Wook Hong, Jae Hyun Park, Justin Zhan. Combined Authentication-Based Multilevel Access Control in Mobile Application for DailyLifeService. *IEEE Transaction on Mobile Computing*. 2010.

[17] Kemal Bicakci, Devrim Unal, Nadir Ascioglu, Oktay Adalier. Mobile Authentication Secure Against Man-In-The-Middle Attacks. *IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*. 2014.

http://doi.org/10.26594/register.v6i1.idarticle

ISSN 2502-3357 (Online)
F. Fulan, et. al./Register 6 (1) 2020 pp. 1-5 ISSN 2503-0477 (Print)

[18] Kyeongwon Choi, Changbin Lee, Woongryul Jeon, Kwangwoo Lee, Dongho Won. A Mobile based Anti-Phishing Authentication Scheme using QR Code. *IEEE International Conference on Mobile IT Convergence*. 2011.

[19] Abdul Rauf, Mahar Faiqurahman, Denar Regata Akbi. Secure Random Port List Generator pada Mekanisme Autentikasi dengan Menggunakan Port Knocking dan Secure Socket Layer. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*. 2018.

[20] Aulia Arif Wardana, Riza Satria Perdana. Access Control on Internet of Things based on Publish/Subscribe using Authentication Server and Secure Protocol. *10th International Conference on Information Technology and Electrical Engineering (ICITEE)*. 2018.

Blockchain-based Two Factor Authentication on Web Application

ORIGINALITY REPORT

11%

SIMILARITY INDEX

PRIMARY SOURCES

1	journal.unipdu.ac.id:8080 Internet	272 words — 6%
2	Kristoforus Fallo, Waskitho Wibisono, Kun Nursyaful Priyo Pamungkas. "Pengembangan mekanisme grid based clustering untuk peningkatan kinerja LEACH pada lingkungan Wireless Sensor Network", Register: Jurnal Ilmiah Teknologi Sistem Informasi, 2019 Crossref	48 words — 1%
3	eprints.umm.ac.id Internet	23 words — 1%
4	Sreenivasa Rao Basavala, Narendra Kumar, Alok Agarrwal. "Authentication: An overview, its types and integration with web and mobile applications", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012 Crossref	22 words — 1%
5	"Blockchain Cybersecurity, Trust and Privacy", Springer Science and Business Media LLC, 2020 Crossref	16 words — < 1%
6	butwhybitcoin.com Internet	14 words — < 1%
7	Hartaman, Aris, Basuki Rahmat, and Istikmal. "Performance and fairness analysis (using Jain's index) of AODV and DSDV based on ACO in MANETs", 2015 4th International Conference on Interactive Digital Media (ICIDM),	14 words — < 1%

2015.
Crossref

8	www.netconfig.co.za Internet	13 words — < 1%
9	Abdulaziz S. Almazyad, Yasir Ahmad. "Chapter 2 A New Approach in T-FA Authentication with OTP Using Mobile Phone", Springer Science and Business Media LLC, 2009 Crossref	8 words — < 1%
10	seecs.nust.edu.pk Internet	8 words — < 1%
11	Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, Mubashir Husain Rehmani. "Applications of Blockchains in the Internet of Things: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, 2019 Crossref	8 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		